aDvens

Security for the greater good

Monthly Cyber Threat Intelligence report
August 2024

2024-09-04 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 38 rue des Jeuneurs - 75002 Paris

Table of content

1. Executive summary

This month, the CERT aDvens presents three noteworthy vulnerabilities, in addition to those already published.

In two articles, CERT analysts present :

- An analysis of the KoreanSpritz implant used by the LAZARUS APT.
- An overview of the activities of hacktivist groups.

2. Vulnerabilities

2.1. CVE-2024-4885

Summoning Team's security researcher Sina Kheirkhah discovered a vulnerability (CVE-2024-4885) in Progress WhatsUp Gold in April 2024. This flaw was patched by the vendor in its June 2024 advisory. Attempts to exploit this vulnerability were subsequently observed by the Shadowserver Foundation starting on 1 August 2024.

An improper file extension validation in the *WhatsUp.ExportUtilities.Export.GetFileWithoutZip* function of Progress WhatsUp Gold allows an unauthenticated attacker, by sending specially crafted HTTP requests, to upload a malicious script and execute it with *iisapppool\nmconsole* privileges.

2.1.1. Type of vulnerability

- CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

2.1.2. Risk

- Remote code execution

2.1.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.1.4. Impacted Products

- Progress WhatsUp Gold versions 2023.1.x prior to 2023.1.3

2.1.5. Recommandations

- Update Progress WhatsUp Gold to version 2023.1.3 or later.
- Additional information is available in Progress' advisory.

2.1.6. Proof of concept

A proof of concept is available in open sources.

2.2. CVE-2024-28986

On 15 August 2024, the CISA added CVE-2024-28986 to its Known Exploited Vulnerabilities Catalog. This vulnerability affects SolarWinds's *Web Help Desk* remote desktop tool, and was originally published on 9 August 2024.

A Java deserialisation flaw in SolarWinds Web Help Desk allows an unauthenticated attacker to execute arbitrary code by sending specially crafted requests.

2.2.1. Type of vulnerability

- CWE-502: Deserialization of Untrusted Data

2.2.2. Risk

- Remote code execution

2.2.3. Severity (base score CVSS 3.1)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.2.4. Impacted Products

- SolarWinds Web Help Desk version 12.8.3 and prior.

2.2.5. Recommandations

- Update SolarWinds Web Help Desk to version 12.8.3 HF 1 or later.
- Additional information is available in SolarWinds' advisory.

2.2.6. Proof of concept

To date, no proof of concept is available in open source.

2.3. CVE-2024-36971

In Android's August security advisory, Google reported that the Android kernel is impacted by CVE-2024-36971, which affects the Linux kernel. It is declared exploited by the editor, who does not attribute it to a specific threat actor.

A memory deallocation flaw in the *__dst_negative_advice()* function of the Linux kernel allows an attacker to execute arbitrary code by sending specially crafted requests.

2.3.1. Type of vulnerability

- CWE-416: Use After Free

2.3.2. Risk

- Remote code execution

2.3.3. Severity (base score CVSS 3.1)

Attack vector	Local	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	Low	Impact on integrity	High
User Interaction	None	Impact on availability	High

2.3.4. Impacted Products

- The Linux kernel versions after 4.6 and prior to 6.9.4

2.3.5. Recommandations

- Update the Linux kernel to version 6.9.4 or later.
- Additional information is available in Linux's advisory.

2.3.6. Proof of concept

To date, no proof of concept is available in open source.

3. Virology : analysis of a NukeSpeed sample - KoreanSpritz (APT Lazarus)

3.1. A new version

Discovered in late June 2024, KoreanSpritz is believed to be a new version of a malware belonging to the NukeSpeed family (aka NukeSpeed and Manuscript): a set of sophisticated backdoors and Trojans that are used by APT Lazarus (North Korea).

Developed in C/C++, the KoreanSpritz backdoor is a portable 32-bit executable for **Microsoft Windows** environments.

KoreanSpritz was allegedly used for cyber-espionage activities against government, financial and industrial entities located in South Korea.

3.2. Features

Below are the main features of the KoreanSpritz malware.

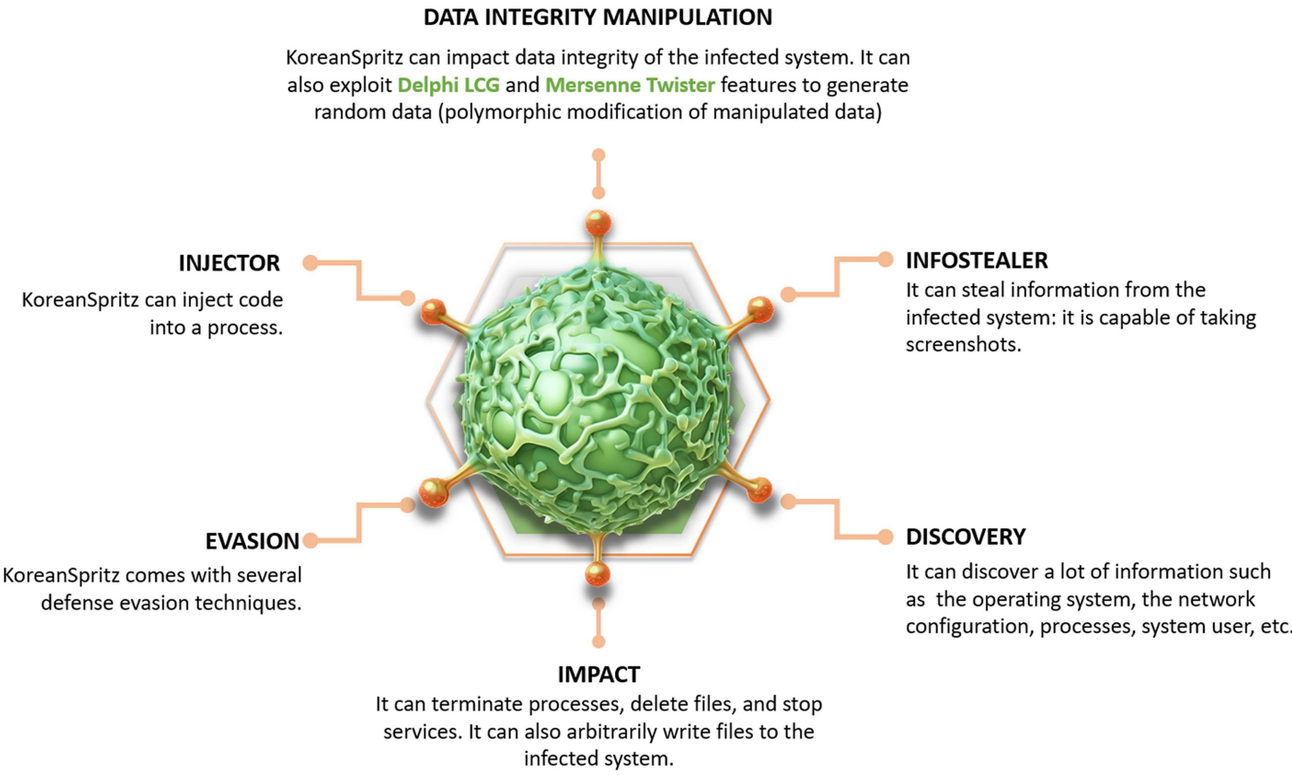

Figure 1. KoreanSpritz features: a multifunction backdoor.

3.3. Victimology

3.3.1. Dissection and analysis of the viral code

Screen Capture

KoreanSpritz can take screenshots by using the **GetDesktopWindow** function.

Functions:

```
GetDesktopWindow (USER32.dll)
CreateCompatibleBitmap (GDI32.dll)
CreateCompatibleDC (GDI32.dll)
BitBlt (GDI32.dll)
```

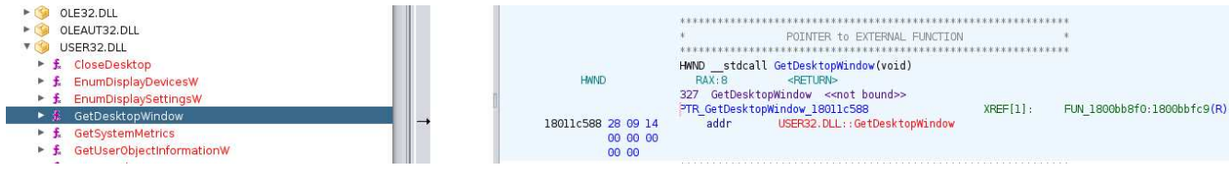

Figure 2. GHIDRA - Code Browsing: function GetDesktopWindow.

Injection

KoreanSpritz appears to be capable of injecting code into a process:

```
Source: C:\Windows\System32\cmd.exe
Processus creation: C:\Windows\System32\rundll32.exe rundll32.exe
"C:\Users\user\Desktop\pconsnap.dll.dll",#1
```

Below are functions used to manipulate memory during the injection:

```
VirtualAlloc (KERNEL32.dll)
VirtualProtect (KERNEL32.dll)
OpenProcess (KERNEL32.dll)
```

Defense evasion: anti-virtualisation

To protect itself against virtualisation, KoreanSpritz searches for certain keywords on the system to check for the presence of a virtual machine:

May try to detect the virtual machine to hinder analysis (VM artifact strings found in memory)	
Source: pconsnap.dll.dll	Binary or memory string: jHGfS
Source: loaddll64.exe, 00000000.00000002.2933846771.000001D16CA38000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000003.2046518335.000001D16CAA4000.00000004.00000020.00020000.00000000.sdmp, loaddll64.exe, 00000000.00000002.2933846771.000001D16CAA4000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.1783305041.000001FC491D3000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000003.1782764478.000001FC491D3000.00000004.00000020.00020000.00000000.sdmp	Binary or memory string: Hyper-V RAW
Source: pconsnap.dll.dll	Binary or memory string: VMcI"!>
Source: rundll32.exe, 00000003.00000003.1782672072.000001FC4921E000.00000004.00000020.00020000.00000000.sdmp, rundll32.exe, 00000003.00000002.1783459795.000001FC49224000.00000004.00000020.00020000.00000000.sdmp	Binary or memory string: Hyper-V RAW@

Figure 3. Anti-virtualisation: keyword search.

KoreanSpritz is able to mark downtime to counter the antiviral analysis:

May sleep (evasive loops) to hinder dynamic analysis	
Source: C:\Windows\System32\loaddll64.exe TID: 7432	Thread sleep time: -120000s >= -30000s

Sample execution stops while process was sleeping (likely an evasion)	
Contains medium sleeps (>= 30s)	
Source: C:\Windows\System32\loaddll64.exe	Thread delayed: delay time: 120000

Figure 4. Anti-virtualisation: keyword research.

Defense evasion: anti-debug

To counter analysis through a disassembler (Reverse engineering), KoreanSpritz manipulates privilege tokens linked to debugging ("debug").

```
Source: C:\Windows\System32\loaddll64.exe
Processus: token adjusted Debug
```

Below is an example of token manipulation:

```
Status: on
Privilege: Debug
State: success or wait
Quantity: 1
Addresse source: 7FFDFB8DD9D6
Symbole: AdjustTokenPrivileges
```

Process Token Activities

Token Adjusted

Status	Privilege	Completion	Count	Source Address	Symbol
on	Debug	success or wait	1	7FFDFB8DD9D6	AdjustTokenPrivileges
on	Take Ownership	success or wait	13	7FFDFB8DDDAE	AdjustTokenPrivileges
on	Take Ownership	success or wait	13	7FFDFB8DE34D	AdjustTokenPrivileges
on	Tcb	not all assigned	203	7FFDFB8DDDAE	AdjustTokenPrivileges

Figure 5. Anti-debug.

Discovery

KoreanSpritz performs discovery by querying registry.

- The system user:

```
Registry key query: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion RegisteredOwner
```

- The date the operating system was installed:

```
Registry key query: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion InstallDate
```

- Microsoft Windows product key:

```
Registry key query: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion ProductId
```

- Globally unique system cryptography identifier:

```
Registry key query: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography MachineGuid
```

- Computer name:

```
Registry key query: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
```

Functions are also used by KoreanSpritz to perform reconnaisance of the network.

- The NetServerEnum function lists all servers of the specified type that are visible in a domain:

```
NetServerEnum (NETAPI32.dll)
```

Communication

On 28 June 2024, KoreanSpritz appears to have communicated with the URL hxxps://www[.]airgreensystem[.]com/DB_command/gallery/bbs_list.php.

Below is an example of communication between KoreanSpritz and **Airgreensystem** :

Timestamp	Bytes transferred	Direction	Data
2024-06-28 08:06:32 UTC	302	OUT	POST /DB_command/gallery/bbs_list.php HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36 Content-Length: 70 Host: www.airgreensystem.com
2024-06-28 08:06:32 UTC	70	OUT	Data Raw: 43 55 37 78 36 3d 45 42 78 77 4e 6e 52 6c 4a 58 4d 45 61 45 68 64 5a 46 64 6e 55 69 4a 69 5a 54 52 34 53 31 42 52 51 31 55 33 65 44 59 78 61 54 51 30 57 6e 46 71 56 57 4e 53 5a 32 45 33 55 6b 78 4f 65 6a 6c 6c Data Ascii: CU7x6=EBxwNnRlJXMEaEhdZFdnUiJiZTR4S1BRQ1U3eDYxaTQ0WnFqVWNSZ2E3UkxOejll
2024-06-28 08:06:33 UTC	420	IN	HTTP/1.1 200 OK Date: Fri, 28 Jun 2024 08:06:32 GMT Server: Apache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Set-Cookie: PHPSESSID=lsvo7qdmn4o8inmvgokvkalfc5; expires=Sat, 29-Jun-2024 08:06:32 GMT; path=/ Upgrade: h2,h2c Connection: Upgrade, close Content-Length: 285 Vary: Accept-Encoding Content-Type: text/html
2024-06-28 08:06:33 UTC	285	IN	Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 20 6d 61 72 67 69 6e 77 69 64 74 68 3d 22 30 22 20 6d 61 72 67 69 6e 68 65 69 67 68 74 3d 22 30 22 20 73 74 79 6c 65 3d 22 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 74 72 61 6e 73 70 61 72 65 6e 74 22 3e 3c 73 63 72 69 70 74 3e 46 44 63 37 56 7a 30 5a 51 67 3d 3d 5a 30 4a 59 4e 46 68 71 4d 51 3d 3d 23 36 35 39 39 31 30 39 30 36 36 39 37 35 37 37 30 35 34 30 30 38 38 35 34 33 32 35 35 36 34 35 30 32 30 30 39 36 36 23 32 33 38 33 33 30 37 34 39 33 32 30 38 36 31 30 31 32 30 37 37 39 38 31 31 30 39 39 38 31 36 36 33 34 34 33 36 31 39 23 32 32 32 34 31 36 34 33 39 30 37 31 33 34 31 35 31 33 30 36 38 30 38 30 37 33 39 34 37 36 37 39 32 Data Ascii: <!DOCTYPE html><html><head></head><body marginwidth="0" marginheight="0" style="background-color:transparent"><script>FDc7Vz0ZQg==Z0JYNFhqMQ==#659910906697577054008854325564502009 66#23833074932086101207798110998166344361 9#222416439071341513068080739476792

Figure 6. Communication between KoreanSpritz and Airgreensystem.

Airgreensystem appears to be a legitimate south-korean organisation.

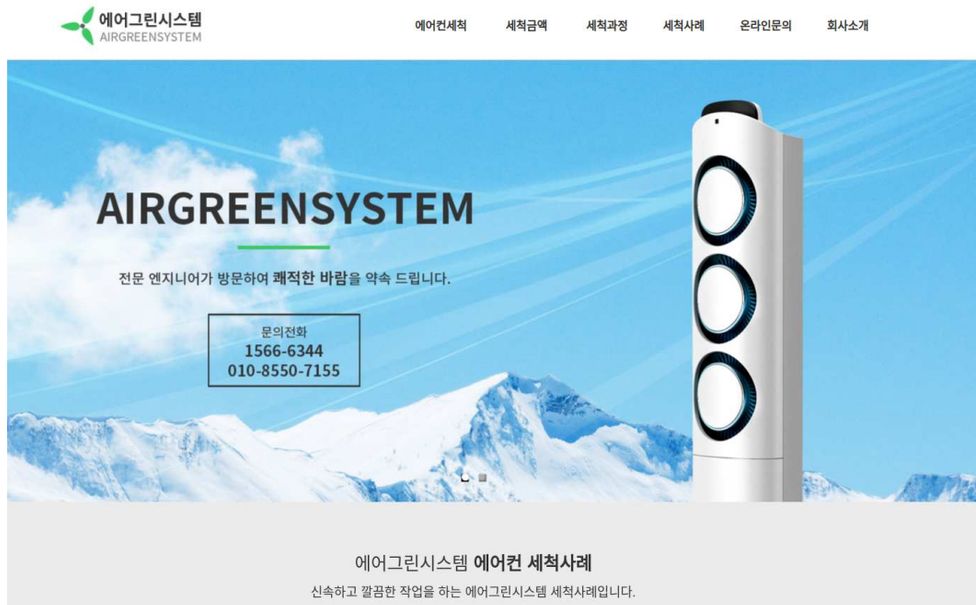

Figure 7. Airgreensystem: a South Korean organisation.

Two URL adresses are discovered in the virus code:

```
hxxp://www[.]komico.or[.]kr/eng/sub3/index8.asp
```

```
hxxp://market[.]gumi.go[.]kr/m/sub1/sub5.asp
```

URL addresses are hardcoded in KoreanSpritz:

```
                    u_http://www.komico.or.kr_18011fd80             XREF[1]:     FUN_1800a63d0:1800a641f(*)
18011fd80 68 00 74      unicode     u"http://www.komico.or.kr"
          00 74 00
          70 00 3a ...

                    u_/eng/sub3/index8.asp_18011fdb0                XREF[1]:     FUN_1800a63d0:1800a644b(*)
18011fdb0 2f 00 65      unicode     u"/eng/sub3/index8.asp"
          00 6e 00
          67 00 2f ...
18011fdda 00            ??          00h
18011fddb 00            ??          00h
18011fddc 00            ??          00h
18011fddd 00            ??          00h
18011fdde 00            ??          00h
18011fddf 00            ??          00h

                    u_http://market.gumi.go.kr_18011fde0            XREF[1]:     FUN_1800a63d0:1800a6477(*)
18011fde0 68 00 74      unicode     u"http://market.gumi.go.kr"
          00 74 00
          70 00 3a ...
18011fe12 00            ??          00h
18011fe13 00            ??          00h
18011fe14 00            ??          00h
18011fe15 00            ??          00h
18011fe16 00            ??          00h
18011fe17 00            ??          00h

                    u_/m/sub1/sub5.asp_18011fe18                    XREF[1]:     FUN_1800a63d0:1800a64a3(*)
18011fe18 2f 00 6d      unicode     u"/m/sub1/sub5.asp"
          00 2f 00
          73 00 75 ...
18011fe3a 00            ??          00h
18011fe3b 00            ??          00h
18011fe3c 00            ??          00h
18011fe3d 00            ??          00h
18011fe3e 00            ??          00h
18011fe3f 00            ??          00h

                    u_https://www.airgreensystem.com_18011fe40      XREF[1]:     FUN_1800a63d0:1800a64cf(*)
18011fe40 68 00 74      unicode     u"https://www.airgreensystem.com"
          00 74 00
          70 00 73 ...
18011fe7e 00            ??          00h
18011fe7f 00            ??          00h

                    u_/DB_command/gallery/bbs_list.php_18011fe80    XREF[1]:     FUN_1800a63d0:1800a64fb(*)
18011fe80 2f 00 44      unicode     u"/DB_command/gallery/bbs_list.php"
          00 42 00
          5f 00 63 ...
```

Figure 8. URL addresses hardcoded within the viral code.

3.4. PCONSNAP.DLL: an interesting detail

Open source research on the keyword **PCONSNAP.DLL** reveals that it was likely used by APT Lazarus from 2022 to 2023.

This article from *Malpedia* indicates that **PCONSNAP.DLL** has been used in the malware PostNapTea (aka SIGNBT)

PostNapTea aka SIGNBT is an HTTP(S) RAT that is written as a complex object-oriented project.

In 2022-2023, it was deployed against targets like a newspaper organization, agriculture-related entity or a software vendor. The initial access was usually achieved by exploiting vulnerabilities in widely-used software in South Korea.

It collects various information about the victim's computer, such as computer name, product name, OS details, system uptime, CPU information, system locale, time zone, network status, and malware configuration.

It stores its configuration in JSON format. It resolves the Windows APIs it requires during runtime, via the Fowler–Noll–Vo (FNV) hash function.

Its internal name in the version-information resource is usually ppcsnap.dll or pconsnap.dll, which loosely inspired its code name.

Figure 9. Source: Malpedia.

The analysed sample from Virus Total is not signed and has the following internal information: Proper Console Snap from Microsoft. This detail is common with PostNapTea.

Signature info

Signature Verification

⚠ File is not signed

File Version Information

Copyright	@ Microsoft Corporation. All rights reserved.
Product	Microsoft@Windows@Operating System
Description	Proper Console Snap
Original Name	pconsnap.dll
Internal Name	pconsnap.dll
File Version	10.0.22000.1

Figure 10. Source: Virus Total.

This detail reinforces the attribution of NukeSpeed - KoreanSpritz to the Lazarus APT.

3.5. NukeSpeed

Below are some samples of NukeSpeed's family.

2019

- Sample: Album.app.zip (19.53 MB) *MAC*
- Detection name: trojan.nukesped/lazarus
- Creation date: Unknown
- First known analysis: October 22, 2019
- SHA256 : d91c233b2f1177357387c29d92bd3f29fab7b90760e59a893a0f447ef2cb4715

2020

- Sample: D2DE01858417FA3B580B3A95857847D5 (164.00 KB) *Windows*
- Detection name: trojan.nukesped/zusy
- Creation date: May 10, 2017
- First known analysis: May 13, 2020
- SHA256 : aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6

2021

- Sample: production.dll (268.50 KB) *Windows*
- Detection name: trojan.nukesped/tigerrat
- Creation date: October 13, 1996
- First known analysis: April 2, 2021
- SHA256 : 0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c

2023

- Sample: 861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d.iso (3.11 MB) *Windows*
- Detection name: Trojan/Win64.NukeSped
- Creation date: Unknown
- First known analysis: May 12, 2023
- SHA256 : 861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d

2024

- Sample: pconsnap.dll or AutoMapper.Net5.dll (71.04 MB) *Windows*
- Detection name: trojan.nukesped/mint
- Creation date: March 28, 2024
- First known analysis: June 25, 2024
- SHA256 : 4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74

3.6. Cluster NukeSpeed

The NukeSpeed family is also known to be the basis of ThreatNeedle which is another family of malware used by Lazarus APT. ThreatNeedle emerged during the year 2019 and brings together backdoors (ThreatNeedle-backdoor) with deployment software (ThreatNeedle-loader).

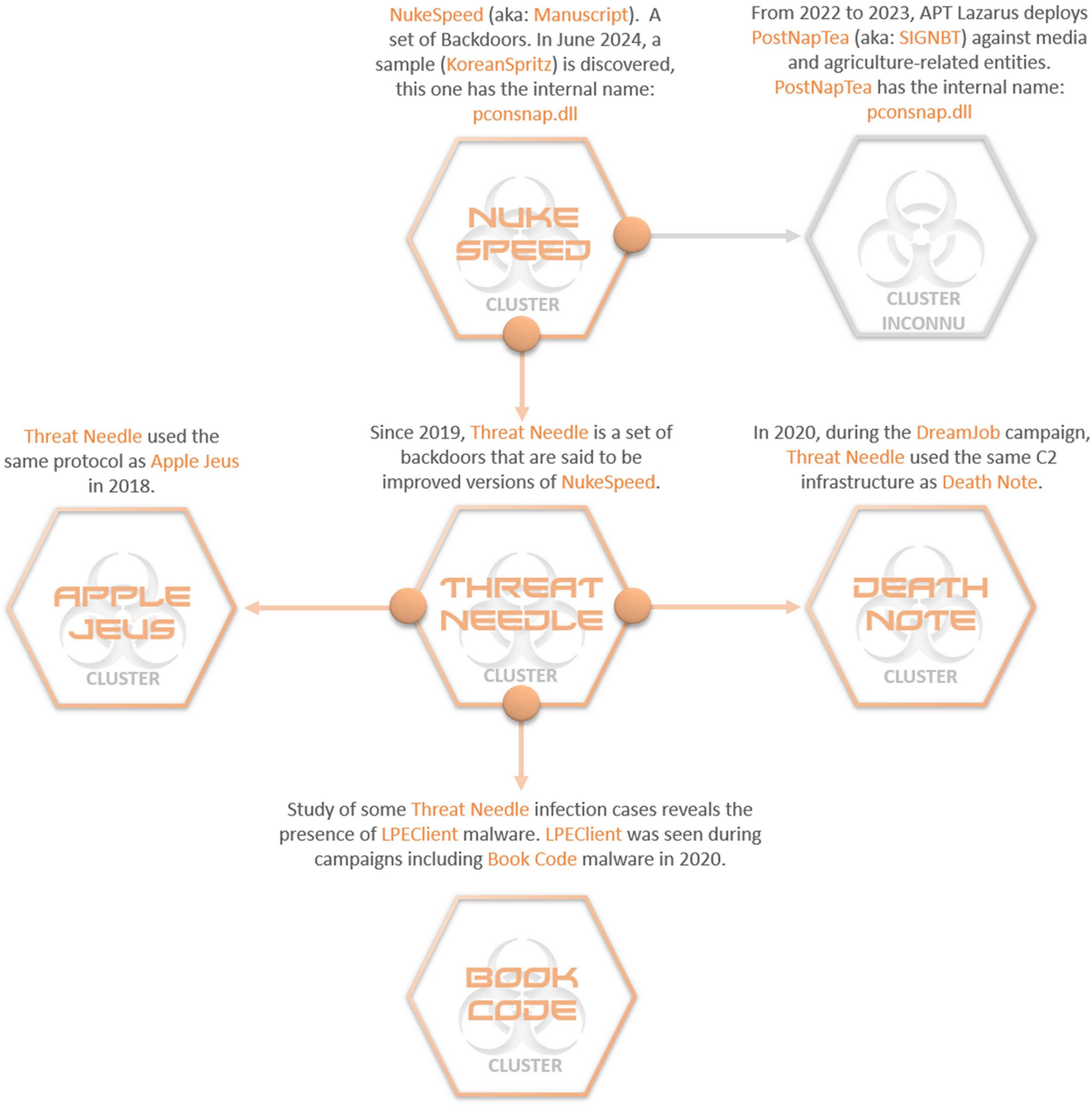

Figure 11. Main clusters surrounding NukeSpeed.

3.7. APT Lazarus - Diamond model

APT Lazarus (aka Dark Seoul, Guardians of Peace, WHOIS Team, Diamond Sleet, Jade Sleet...) is an North Korean advanced and persistent threat.

Figure 12. APT Lazarus diamond model.

3.8. MITRE ATT&CK

RESOURCE DEVELOPMENT

T1587.001 Develop Capabilities: Malware.

EXECUTION

T1129 Shared Modules. T1059 Command and Scripting Interpreter.
T11569.002 System Services: Service Execution.

PERSISTENCE

T1574.002 DLL Side-loading. T1543 Create or Modify System Process.
T1134 Access Token Manipulation.

PRIVILEGE ESCALATION

T1055 Process Injection. T1548 Abuse Elevation Control Mechanism. T1574.002 DLL Side-loading.
T1134 Access Token Manipulation. T1134.004 Access Token Manipulation: Parent PID Spoofing.

DEFENSE EVASION

1055 Process Injection. T1548 Abuse Elevation Control Mechanism. T1574.002 DLL Side-loading. T1218.011 RunDLL32. T1497 Virtualization / Sandbox Evasion. T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion. T1134 Access Token Manipulation. T1134.004 Access Token Manipulation: Parent PID Spoofing. T1027.005 Obfuscated Files or Information. T1127 Trusted Developer Utilities Proxy Execution. . T1027 Obfuscated Files or Information: Software Packing. T1036.007 Masquerading: Double File Extension.

DISCOVERY

T1135 Network Share Discovery. T1082 System Information Discovery. T1518.001 Software Discovery: Security Software Discovery. T1518.016 System Network Configuration Discovery. T15049 System Network Connections Discovery. T1033 System Owner/User Discovery. T1007 System Service Discovery. T1124 System Time Discovery. T1016.001 System Network Configuration Discovery: Internet Connection Discovery. T1083 File and Directory Discovery. T1497 Virtualization / Sandbox Evasion. T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion. T1012 Query Registry.

COLLECTION

T1113 Screen Capture. T1005 Data from Local System (Parse credit card information + Get geographical location).

COMMAND AND CONTROL

T1071 Application Layer Protocol. T1573 Encrypted Channel. T1095 Non-Application Layer Protocol.

IMPACT

T1565 Data Manipulation. T1491 Defacement. T1489 Service Stop.

Figure 13. TTPS KOREANSPRITZ (APT LAZARUS)

3.9. IOCs

Detection name of the NukeSpeed sample - KoreanSpritz 2024: TR/NukeSped.dggcy (Avira), Win64/NukeSped.KP trojan (Hybrid Analysis), Trojan:Win64/NukeSped.d298f49d (Alibaba), Trojan/Win.Lazardoor.R592967 (Ahnlab).

3.9.1. IOC NukeSpeed - KoreanSpritz 2024

TLP	TYPE	VALUE	COMMENTARY
TLP:CLEAR	SHA256	4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74	NukeSpeed-KoreanSpritz Backdoor
TLP:CLEAR	SHA1	2816b44de0065bee18ac963bcc3bf9b195499eeb	NukeSpeed-KoreanSpritz Backdoor
TLP:CLEAR	MD5	8fb5e72a31680189d9a529b49962a0b1	NukeSpeed-KoreanSpritz Backdoor
TLP:CLEAR	URL	hxxp://www[.]komico.or[.]kr/eng/sub3/index8.asp	Compromised URL
TLP:CLEAR	URL	hxxp://market[.]gumi.go[.]kr/m/sub1/sub5.asp	Compromised URL
TLP:CLEAR	URL	hxxps://www[.]airgreensystem[.]com/DB_command/gallery/bbs_list.php	Compromised URL (maybe C2)

3.9.2. IOC NukeSpeed - older variants

TLP	TYPE	VALUE	COMMENTARY
TLP:CLEAR	Artefact	Album.app.zip	NukeSpeed 2019
TLP:CLEAR	SHA256	d91c233b2f1177357387c29d92bd3f29fab7b90760e59a893a0f447ef2cb4715	NukeSpeed 2019
TLP:CLEAR	SHA1	5955837b6f888a733e05cbb444279d24f5313ac5	NukeSpeed 2019
TLP:CLEAR	MD5	a8096ddf8758a79fdf68753190c6216a	NukeSpeed 2019
TLP:CLEAR	Artefact	D2DE01858417FA3B580B3A95857847D5	NukeSpeed 2020
TLP:CLEAR	SHA256	aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6	NukeSpeed 2020
TLP:CLEAR	SHA1	2c879a1d4b6334c59ac5f11c2038d273d334befe	NukeSpeed 2020
TLP:CLEAR	MD5	d2de01858417fa3b580b3a95857847d5	NukeSpeed 2020
TLP:CLEAR	IP	112(.)217.108.138	NukeSpeed 2020
TLP:CLEAR	Artefact	production.dll	NukeSpeed 2021
TLP:CLEAR	SHA256	0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c	NukeSpeed 2021
TLP:CLEAR	SHA1	98d6417addec8607f1b62cc52123be76424befc0	NukeSpeed 2021
TLP:CLEAR	MD5	f4d46629ca15313b94992f3798718df7	NukeSpeed 2021
TLP:CLEAR	Artefact	861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d.iso	NukeSpeed 2023
TLP:CLEAR	SHA256	861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d	NukeSpeed 2023
TLP:CLEAR	SHA1	d2f160bf01a1f7b863188c9b953c197f7b876c7a	NukeSpeed 2023
TLP:CLEAR	MD5	4e10c8d3d71136e870cf58c0e31db2bc	NukeSpeed 2023

3.10. YARA

3.10.1. YARA 1

YARA - aDvens

```
rule KOREANSPRITZ_Specific_strings {
meta:
author = "ADVENS CTI"
date = "3/07/2024"
source = "ADVENS"
status = "RELEASED"
sharing = "TLP:CLEAR"
malware = "NUKESPEED_variant_KOREANSPRITZ"
description = "Yara_rule_that_detects_KOREANSPRITZ_backdoor."
info = "KOREANSPRITZ_Backdoor"
Sample_SHA256 = "4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74"
Sample_SHA1 = "2816b44de0065bee18ac963bcc3bf9b195499eeb"
Sample_MD5 = "8fb5e72a31680189d9a529b49962a0b1"
//Vérification hexadécimale
strings:
$Hexa1 = { 56 18 48 8b c2 48 2b c1 }
$Hexa2 = { 48 89 85 58 01 00 00 48 }
$Hexa3 = { 48 89 5c 24 70 48 8d 54 }
$Hexa4 = { 49 ff c0 66 42 83 3c 40 }
$Hexa5 = { f6 ff 48 8d 85 28 07 00 }
$Hexa6 = { 48 63 c2 48 8d 4c 24 20 }
$Hexa7 = { 5c 0d 05 00 33 d2 38 45 }
$Hexa8 = { e8 7b 2d 00 00 cc cc cc }
//Vérification des fonctions
$Add1 = "GetDesktopWindow"
$Add2 = "DeleteFileW"
$Add3 = "CreateFileW"
$Add4 = "NetServerEnum"
$Add5 = "OpenInputDesktop"
$Add6 = "TerminateProcess"
condition:
filesize > 74490000 and filesize < 74500000 and all of ($Hexa*) and 3 of ($Add*)
}
```

3.10.2. YARA 2

YARA - FIleScan.IO

Source: https://www.filescan.io/uploads/667e6d880bf5978c0b1318c1/reports/2c045983-2ef5-4dc3-9f87-a68de8b27d23/overview

```
    rule autogen_peexe_FingerprintLolbinMasqueradeOverlayPackedRemote_4f9ef9f4
    {
    meta:
    author = "FileScan.IO Engine v1.1.0-6f9b172"
    date = "2024-06-28"
    sample = "4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74"
    score = 75
    tags = "fingerprint,lolbin,masquerade,overlay,packed,remote"
    isWeakRule = true
    strings:
    //IOC patterns
    $req0 = "http://market.gumi.go.kr"
    $req1 = "http://www.komico.or.kr"
    $req2 = "https://www.airgreensystem.com"
    //optional strings
    $opt0 = "!\"#$%&'()*+,-
./0123@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@@@@@@@"
    $opt1 = "ADVAPI32.dll"
    $opt2 = "AcquireSRWLockExclusive"
    $opt3 = "AreFileApisANSI"
    $opt4 = "CloseDesktop"
```

```
        $opt5 = "CreateFileA"
        $opt6 = "CreateFileMappingW"
        $opt7 = "CreateFileW"
        $opt8 = "CreateThread"
        $opt9 = "DecodePointer"
        $opt10 = "DeleteCriticalSection"
        $opt11 = "DeleteFileW"
        $opt12 = "DeleteIpNetEntry"
        $opt13 = "DeleteProcThreadAttributeList"
        $opt14 = "DeleteService"
        $opt15 = "EncodePointer"
        $opt16 = "EnterCriticalSection"
        $opt17 = "EnumDependentServicesW"
        $opt18 = "EnumDisplayDevicesW"
        $opt19 = "EnumServicesStatusExW"
        $opt20 = "EnumSystemLocalesEx"
        $opt21 = "EnumSystemLocalesW"
        $opt22 = "ExitProcess"
        $opt23 = "FileTimeToSystemTime"
        $opt24 = "FindFirstFileExW"
        $opt25 = "FindNextFileW"
        $opt26 = "FlushFileBuffers"
        $opt27 = "FreeEnvironmentStringsW"
        $opt28 = "FreeLibrary"
        $opt29 = "GetCommandLineA"
        $opt30 = "GetCommandLineW"
        $opt31 = "GetComputerNameA"
        $opt32 = "GetComputerNameW"
        $opt33 = "GetConsoleMode"
        $opt34 = "GetConsoleOutputCP"
        $opt35 = "GetCurrentProcess"
        $opt36 = "GetCurrentProcessId"
        $opt37 = "GetCurrentThreadId"
        $opt38 = "GetDateFormatW"
        $opt39 = "GetDesktopWindow"
        $opt40 = "GetEnvironmentStringsW"
        $opt41 = "GetFileAttributesExW"
        $opt42 = "GetFileInformationByHandle"
        $opt43 = "GetFileSize"
        $opt44 = "GetFileSizeEx"
        $opt45 = "GetFileType"
        $opt46 = "GetLastError"
        $opt47 = "GetLocalTime"
        $opt48 = "GetLocaleInfoW"
        $opt49 = "GetModuleFileNameW"
        $opt50 = "GetModuleHandleExW"
        $opt51 = "GetModuleHandleW"
        $opt52 = "GetProcAddress"
        $opt53 = "GetProcessHeap"
        $opt54 = "GetProcessId"
        $opt55 = "GetServiceDisplayNameW"
        $opt56 = "GetServiceKeyNameW"
        $opt57 = "GetStartupInfoW"
        $opt58 = "GetStdHandle"
        $opt59 = "GetStringTypeW"
        $opt60 = "GetSystemInfo"
        $opt61 = "GetSystemMetrics"
        $opt62 = "GetSystemTimeAsFileTime"
        $opt63 = "GetTickCount"
        $opt64 = "GetTickCount64"
        $opt65 = "GetTimeFormatW"
        $opt66 = "GetTimeZoneInformation"
        $opt67 = "GetUserDefaultLCID"
        $opt68 = "GetUserObjectInformationW"
        $opt69 = "GetWindowsDirectoryW"
        $opt70 = "GlobalAlloc"
        $opt71 = "GlobalFree"
        $opt72 = "GlobalLock"
        $opt73 = "GlobalUnlock"
        $opt74 = "HeapReAlloc"
        $opt75 = "IPHLPAPI.DLL"
        $opt76 = "InitializeCriticalSectionAndSpinCount"
        $opt77 = "InitializeCriticalSectionEx"
        $opt78 = "InitializeProcThreadAttributeList"
        $opt79 = "InitializeSListHead"
        $opt80 = "InterlockedFlushSList"
        $opt81 = "IsBadReadPtr"
        $opt82 = "IsDebuggerPresent"
        $opt83 = "IsProcessorFeaturePresent"
        $opt84 = "KERNEL32.dll"
        $opt85 = "LCMapStringW"
        $opt86 = "LeaveCriticalSection"
        $opt87 = "LoadLibraryA"
```

```
    $opt88 = "LoadLibraryExW"
    $opt89 = "LoadLibraryW"
    $opt90 = "LocalAlloc"
    $opt91 = "LocalReAlloc"
    $opt92 = "LockServiceDatabase"
    $opt93 = "LookupAccountSidW"
    $opt94 = "MapViewOfFile"
    $opt95 = "MoveFileExW"
    $opt96 = "NETAPI32.dll"
    $opt97 = "NetConnectionEnum"
    $opt98 = "NetServerEnum"
    $opt99 = "OLEAUT32.dll"
    $opt100 = "OpenDesktopW"
    $opt101 = "OpenInputDesktop"
    $opt102 = "OpenProcess"
    $opt103 = "OpenWindowStationW"
    $opt104 = "QueryPerformanceCounter"
    $opt105 = "QueryPerformanceFrequency"
    $opt106 = "QueryServiceStatus"
    $opt107 = "RaiseException"
    $opt108 = "ReadConsoleW"
    $opt109 = "ReleaseSRWLockExclusive"
    $opt110 = "RtlCaptureContext"
    $opt111 = "RtlLookupFunctionEntry"
    $opt112 = "RtlPcToFileHeader"
    $opt113 = "RtlVirtualUnwind"
    $opt114 = "SeDebugPrivilege"
    $opt115 = "SetEndOfFile"
    $opt116 = "SetEnvironmentVariableW"
    $opt117 = "SetFilePointer"
    $opt118 = "SetFilePointerEx"
    $opt119 = "SetLastError"
    $opt120 = "SetProcessWindowStation"
    $opt121 = "SetStdHandle"
    $opt122 = "SetThreadDesktop"
    $opt123 = "SetUnhandledExceptionFilter"
    $opt124 = "SleepConditionVariableSRW"
    $opt125 = "Status       Local     Remote                    Network"
    $opt126 = "SystemTimeToFileTime"
    $opt127 = "TerminateProcess"
    $opt128 = "TlsGetValue"
    $opt129 = "TlsSetValue"
    $opt130 = "USER32.dll"
    $opt131 = "UnhandledExceptionFilter"
    $opt132 = "UnmapViewOfFile"
    $opt133 = "UpdateProcThreadAttribute"
    $opt134 = "VirtualAlloc"
    $opt135 = "VirtualFree"
    $opt136 = "VirtualProtect"
    $opt137 = "WS2_32.dll"
    $opt138 = "WaitForSingleObject"
    $opt139 = "WakeAllConditionVariable"
    $opt140 = "WriteConsoleW"
    $opt141 = "connection reset"
    $opt142 = "gdiplus.dll"
    $opt143 = "mscoree.dll"
    $opt144 = "network reset"
    $opt145 = "read only file system"
    $opt146 = "shlwapi.dll"
    $opt147 = "stream timeout"
    condition:
    //require 50% of optional strings
    uint16(0) == 0x5A4D and filesize > 67045479 and filesize < 81944473 and all of ($req*) and 74 of ($opt*)
}
```

4. Hacktivist groups: an overview

The political events of 2023 and 2024 gave rise to a large number of hacktivist groups in early 2024. While this type of group has existed for many years (Anonymous, Caliphate Cyber Army), the use of offensive cyber actions by civilians has become an integral part of current geopolitical crises.

A survey of hacktivist groups in the second quarter of 2024 highlights the shifts that have taken place over time. We can see the emergence of new major players and the disappearance or dormancy of others.

For example, Anonymous Sudan and Killnet, which were omnipresent at the start of the war in Ukraine, have given way to new players such as the Holy League and NoName057.

In addition, the media resonance of the war waged by the Israeli state in the Gaza Strip following the attack on 7 October 2023 gave rise in early 2024 to the creation of numerous pro-Palestinian hacktivist groups from several countries, allying themselves in the manner of an international cyber brigade or legion.

In line with these initial observations, hacktivist groups can now be divided into two main families based on the two main geopolitical issues of the day: the Israeli-Palestinian conflict and the Russian-Ukrainian war.

4.1. Hacktor's profiles

4.1.1. NoName057(16)

This hacktivist group emerged in March 2022 as part of the war in Ukraine. It is currently the largest collective and is responsible for 36% of all DDOS attacks against Ukraine. A distant second is Anonymous Russia, responsible for 17% of these attacks.

The collective has succeeded in attracting a large contingent of volunteers thanks to a number of factors:

- extensive communication through its Telegram channels,
- the creation of a specific channel for English-speaking volunteers,
- simplified procedures to help volunteers get up and running quickly, with tutorials,
- the provision of the *DDOSIA* software kit and technical support.

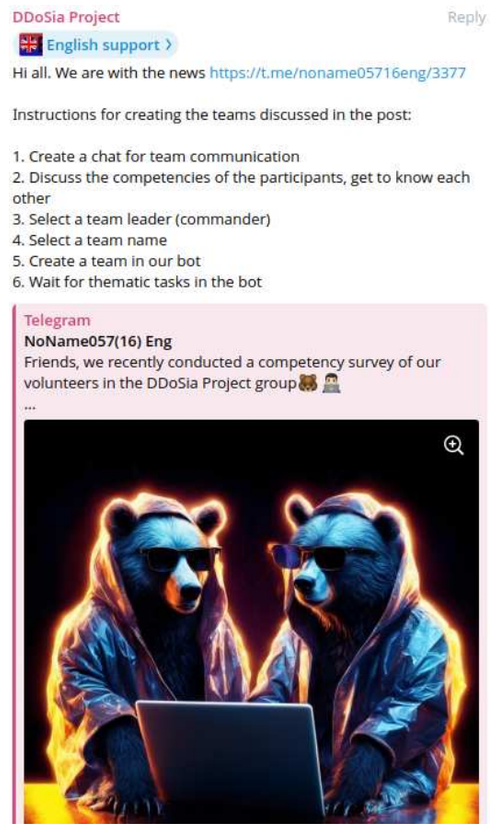

Figure 14. NoName057(16) recruitment tutorial - Telegram

Finally, the collective is known for paying its most active volunteers in cryptocurrency.

4.1.2. Rippersec

Hailing from Malaysia, Rippersec is a perfect example of the globalisation of hacktivism specific to the Israeli-Palestinian conflict. In the minds of these groups, the theme of the Ummah (community of believers) is a recurring one, naturally leading them to form alliances.

The group's main motivation is to support the Palestinian cause and to target organisations or governments perceived as favourable to Israel. Rippersec currently stands out for being at the forefront of current attacks on French websites in reaction to the arrest of Pavel Durov at Le Bourget. The group has carried out DDOS attacks against the Police nationale website.

Figure 15. RipperSec claim - Telegram

4.2. Alliances

Over the course of the Ukrainian conflict, alliances were formed, notably between pro-Russian hacktivist groups who formed the Killnet alliance, a collective that marked the first years of the wars. A new collective was formed in May 2024. Its aim is to attack European countries and NATO members. It has around twenty members.

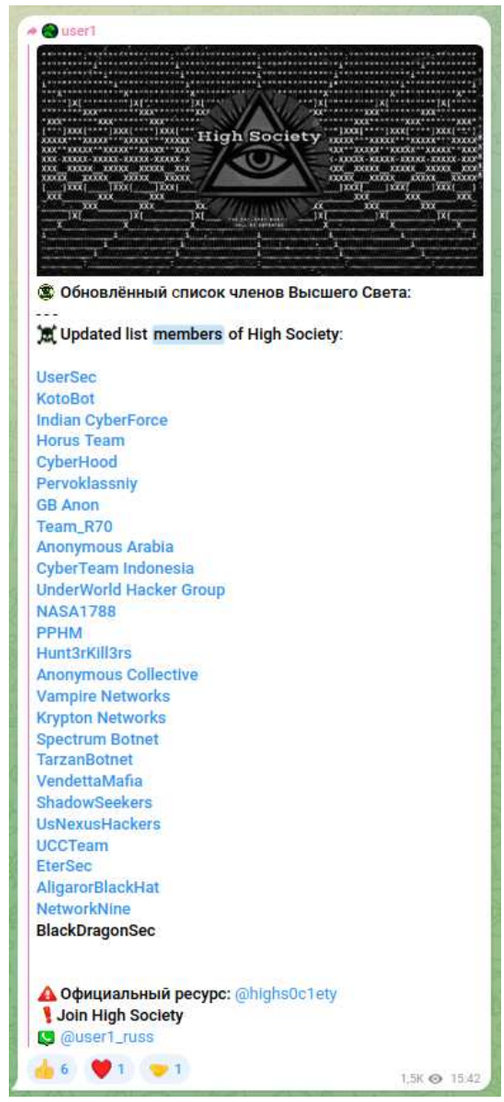

Figure 16. High Society Members - Telegram

On 29 June 2024, a new coalition of pro-Palestine hacktivist groups was created, bringing together 35 collectives: *October 7th alliance*.

#Anonymous_Arabs
#Hack_Force
#Black_Maskers_Army
#CyberVolk
#ISLAMIC_CYBER_TEAM_INDONESIA
#Lulzsec_Indonesia
#TOXCAR_CYBER_TEAM
#Cryptaris
#cYBER_TEAM_INDONESIA
#BIOCRYPT_COMMUNITY
#Evil_of_Anti_ddos
#CRYPTO_CORP
#dark_spot
#ANON_SEC_BD
#NulSec
#ghostsofcl
#RCH_SEC
#cyber_stine
#Хактивистский_Советский_Союз
#SYLIIETGANG_SG
#Team_Arxu
#Team_1945
#Anonymous
#Team_insane_Pakistan
#Anonymous_Palestine
#Ketapang_Grey_Hat_Team
#BEN_MHIDI_54
#Anonymous_SYRIA
#Anonymous_KSA
#Anonymous_DZ
#YEMEN_GOST
#Team_Y_S_G
#EVIL_BYTE
#Lulzec_Black
#Moroccan_Soldiers

All group union

Figure 17. October 7th alliance members - Telegram

On 22 July 2024, these two coalitions with opposing profiles and similar goals decided to merge: the Holy League was created. The organisation claims to have more than 80 groups, some of which are secretly part of the alliance. 69 have been made official and are represented in the alliance's Telegram channel.

Figure 18. Announcement of the creation of the Holy League - Telegram

the Holy League has also claimed responsibility for attacks on France over the arrest of Pavel Durov, and the hashtag #FreeDurov is currently being used by a large number of hacktivist groups of very different persuasions.

4.3. Techniques

4.3.1. DDOS & Defacement

These harassment techniques are widely used, as they require less technical knowledge. DDOS consists of rendering a service unusable by flooding it with requests aimed at bringing down its servers, while defacement aims to change the appearance of a website in order to display its own message. The use of these techniques has above all a symbolic and media impact, which is the goal of hacktivism: to show off and humiliate the adversary.

Figure 19. Defacement of Israeli websites by ByteBlitz Team and Cyb3r Drag0nz - Telegram

4.3.2. Information theft, doxing

Doxing is the most violent form of hacktivism, involving the publication of personal data about an individual. At the beginning of the invasion of the Gaza Strip and the attempted bombing by Iran, a strong radicalisation was observed in several hacktivist groups with a blurring of the boundaries between physical and cyber conflicts.

In this case, cyber action serves as a preparation ground for physical operations, doxing with a view to assassination, calls for terrorist operations, theft of sensitive data for strikes, and so on. A new stage has been reached in this intensity, with hacktivist operations becoming the cyber brick of an asymmetric physical war.

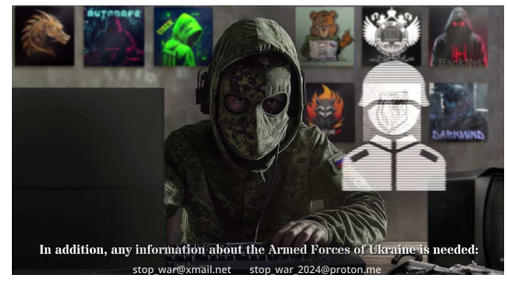

Figure 20. Call for intelligence on Ukrainian military personnel and infrastructure by NoName057(16) - Telegram

4.3.3. Propaganda or disinformation campaigns

The field of psychological warfare is part of the range of operations carried out by hacktivists, but is somewhat removed from their core activities. Psychological actions in the cyber field are a separate subject with many ramifications. The groups mentioned

previously may however publish material with this aim in order to promote themselves or justify their attacks.

The Ghost of Palestine group uses its broadcasting channels to wage a propaganda war on Israeli military actions, amplifying stories of Palestinian resistance or highlighting the victims of bombardments in order to remotivate public opinion and justify its actions.

Figure 21. Anti-Israeli propaganda video published by Ghosts of Palestine

```
Translation of the post: 'When these missiles are launched on the temporary entity, O God, hasten to destroy
the oppressors, our Lord, and accept that you are the one who hears supplication, and your Lord said, "Call
on me and I will answer you" Do not be arrogant about the worship of supplication is very important, the way
of the prophets to speak with God, so call on Him through them, and avoid those who blaspheme His names,
they will reward what they have done.'
```

4.4. Tools

Hacktivists use botnets to carry out their attacks. Some specifically exploit Mirai. Other groups have enough members and allies to build up their fleets by making machines available on a voluntary basis. These networks then use specific tools to coordinate their attacks.

4.4.1. DDOSIA

The core of NoName057's operation is based on the distribution of the DDOSIA tool. NoName057 recruits volunteers via Telegram: once they have registered for the DDOSIA project, new members receive a software kit and a tutorial on how to install DDOSIA via a bot. A support channel in English is also available for technical assistance.

Developed in Python, DDoSia is capable of running on several platforms (Windows, Linux, macOS) and exploits the computing power of participating computers to overwhelm targets with requests. Each machine is identified by a unique GUID (for Windows environments extracted from the registry) and data is transmitted in encrypted form, making it difficult to trace participants. The tool connects to command and control (C2) servers to coordinate the attacks. These servers are regularly changed to avoid being blocked.

4.4.2. MEGAMEDUSA

The RipperSec group uses Megamedusa software for its DDOS attacks, a tool developed in-house and available on Github. MegaMedusa is currently at version 3.2.

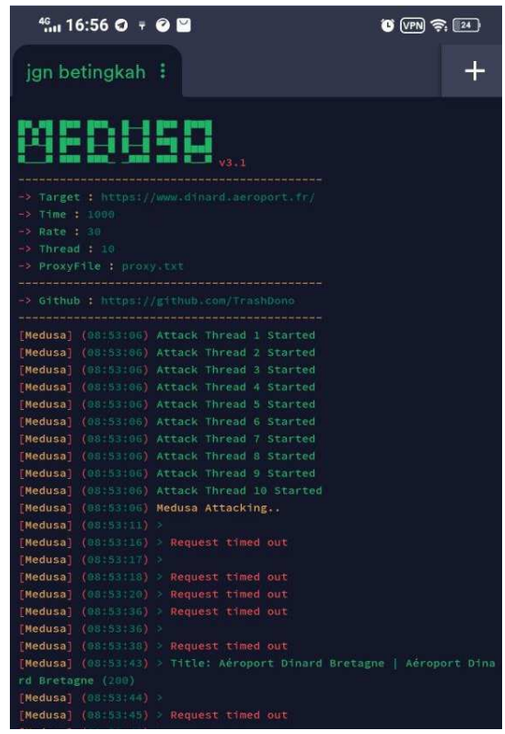

Figure 22. DDOS of Dinard airport via MegaMedusa - Telegram

The software enables HTTP or HTTPS requests to be sent in bulk, and has features for bypassing CAPTCHAs or protection systems such as Cloudflare.

Figure 23. RipperSec offers free access to MegaMedusa - Telegram

However, the tool seems to be limited, and it would appear that the consumer version is more limited than the tool used internally.

4.4.3. LOIC & HOIC

Low Orbit Ion Cannon (LOIC) and its new High Orbit Ion Cannon (HOIC) versions are the most widely used open source DDoS tools, often used by hacktivists to overwhelm a server with HTTP, UDP or TCP requests. HOIC has a user interface that makes it accessible to novices and can host custom scripts designed to amplify an attack. HOIC is used by groups such as Anonymous and the pro-Ukrainian hacktivist collective HackYourMom.

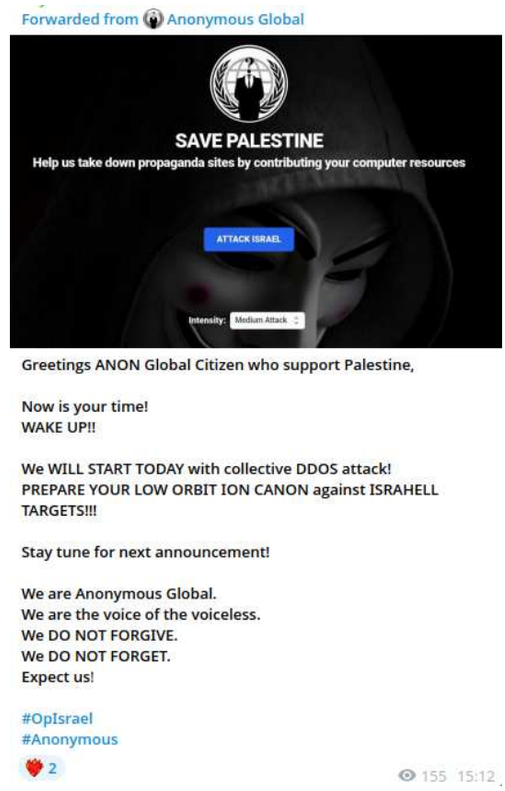

Figure 24. Message from Anonymous Global claiming use of LOIC- Telegram

Other tools are also used, such as Memcrashed, a tool for sending UDP packets to MemCached servers using the Shodan API. Finally, we should mention SlowLoris: a script that enables server DOS from a single machine via a low number of incomplete requests that prevent connections from being closed. This was the first tool to use this type of attack, which is now widely used by LOIC and HOIC.

Figure 25. Tool recommendations from the pro-Palestinian group Team 1945 - Telegram

4.5. CONCLUSION

The activity of hacktivist groups is set to grow, generating new opportunities such as the development of DDOS as a service as practised by Dark Storm Team or the group Doubleface, a member of the Holy League.

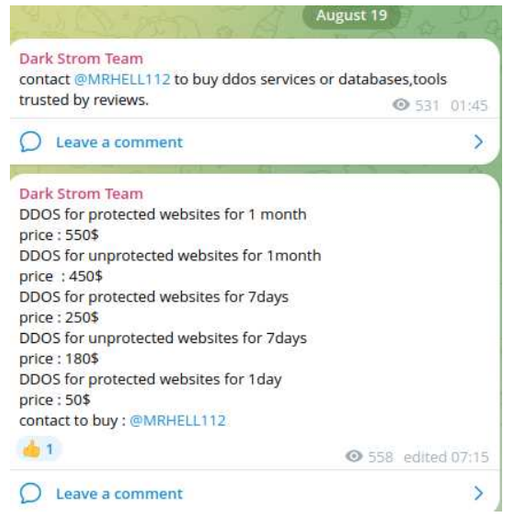

Figure 26. Pricing DDOS as a service - Dark Storm Team - Telegram

Depending on how conflicts evolve, radicalisation may be feared among certain groups who no longer wish to limit themselves to symbolic operations. These activities are moving away from the traditional hacktivist framework towards that of guerrilla warfare.

In this way, the emergence of these small-scale cyber operations by private groups can be compared to the advent of commercial FPV drones in the Ukrainian conflict: a new asymmetric combat technique generated by a form of uberisation of warfare.

5. Sources

CVE-2024-28986

- https://nvd.nist.gov/vuln/detail/CVE-2024-28986
- https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28986
- https://www.cisa.gov/news-events/alerts/2024/08/15/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.helpnetsecurity.com/2024/08/15/cve-2024-28986/

CVE-2024-4885

- https://nvd.nist.gov/vuln/detail/CVE-2024-4885
- https://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-June-2024
- https://summoning.team/blog/progress-whatsup-gold-rce-cve-2024-4885/
- https://x.com/Shadowserver/status/1821121075704647731
- https://thehackernews.com/2024/08/critical-security-flaw-in-whatsup-gold.html
- https://www.bleepingcomputer.com/news/security/critical-progress-whatsup-rce-flaw-now-under-active-exploitation/

CVE-2024-36971

- https://nvd.nist.gov/vuln/detail/CVE-2024-36971
- https://source.android.com/docs/security/bulletin/2024-08-01?hl=fr
- https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=92f1655aa2b2294d0b49925f3b875a634bd3b59e
- https://therecord.media/android-zero-day-google-fix-august-patch
- https://thehackernews.com/2024/08/google-patches-new-android-kernel.html

NUKESPEED - KOREANSPRITZ (APT LAZARUS)

- https://www.joesandbox.com/analysis/1464042/0/html
- https://bazaar.abuse.ch/sample/4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74/
- https://www.virustotal.com/gui/file/4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74/community
- https://cyber-fortress.com/docs/result/index.php?id=667e6dc27d0a7ff58bc74e3fwin10vpnfull_triage
- https://www.abuseipdb.com/check/211.47.74.11
- https://tria.ge/240628-jvzv4syeqb
- https://www.airgreensystem.com/index.html?menu=qlist1&dbname=oqbbs01
- https://www.google.com/maps/place/19-3+Jindeung-ro+19beon-gil,+Euijeongbu,+Gyeonggi-do,+Cor%C3%A9e+du+Sud/@37.7596224,127.028956,17z/data=!3m1!4b1!4m6!3m5!1s0x357cc12831a53295:0xdda7e5d50b75d3ed!8m2!3d37.7596224!4d127.0315309!16s%2Fg%2F11bz7d0dw2?hl=fr-FR&entry=ttu
- https://box.zero.camp/analysis/51384/summary/
- https://x.com/asdasd13asbz/status/1806561339604877609?t=RLQPn-uhVdUHo7DykjUrOg&s=19
- https://securelist.com/lazarus-threatneedle/100803/
- https://securelist.com/operation-applejeus/87553/
- https://threatpost.com/lazarus-targets-defense-threatneedle-malware/164321/
- https://malpedia.caad.fkie.fraunhofer.de/details/win.postnaptea

NUKESPEED (APT LAZARUS)

Variant 2019

- https://www.pcrisk.fr/guides-de-suppression/9478-nukesped-trojan-mac
- https://www.virustotal.com/gui/file/d91c233b2f1177357387c29d92bd3f29fab7b90760e59a893a0f447ef2cb4715/community

Variant 2020

- https://bazaar.abuse.ch/sample/aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6/
- https://www.virustotal.com/gui/file/aab2868a6ebc6bdee5bd12104191db9fc1950b30bcf96eab99801624651e77b6

Variant 2021

- https://bazaar.abuse.ch/sample/0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c/
- https://www.virustotal.com/gui/file/0996a8e5ec1a41645309e2ca395d3a6b766a7c52784c974c776f258c1b25a76c/

Variant 2023

- https://bazaar.abuse.ch/sample/861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d/
- https://www.virustotal.com/gui/file/861a0b52b3676fb46f4d97699cd3dc02f2f8b5964633491f61a8b22ce9221b1d/

Variant 2024 (KoreanSPritz)

- https://bazaar.abuse.ch/sample/4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74/
- https://www.virustotal.com/gui/file/4f9ef9f4b90d8e0928a36369e90d912b1f4a3b5afc173cddecb1790aa06cdc74/

HACKTIVISM

- Principal sources : Telegram Channels and Groups

Profiles

- https://socradar.io/dark-web-profile-noname05716/
- https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/rising-from-the-underground-hacktivism-in-2024

Tools

- https://www.radware.com/blog/uncategorized/2024/08/megamedusa-rippersec-public-web-ddos-attack-tool/?&web_view=true